**International Journal of Electronics,
Communication & Instrumentation Engineering
Research and Development (IJECIERD)
ISSN(P): 2249-684X; ISSN(E): 2249-7951
Vol. 4, Issue 2, Apr 2014, 1-4**
© TJPRC Pvt. Ltd.

TRANS STELLAR
• Journal Publications • Research Consultancy

NETWORK SECURITY WITH QUANTUM CRYPTOGRAPHY – A REVIEW

KRANTISH V. POL & D. J. PETHE

Department of Electronics and Telecommunications, Datta Meghe College of Engineering,

Airoli, Navi Mumbai, Maharashtra, India

ABSTRACT

In today's so called modern World, most digital networks rely on classical cryptosystems (CC) to secure the confidentiality and integrity of traffic carried across the network. However, these classical schemes for key distribution rely on the unproven computational assumptions and hence keys can be easily compromised in many ways. Quantum cryptography (QC) is an emerging approach to secure communications by applying the phenomena of quantum physics. Unlike classical or current cryptosystems, which uses mathematical techniques to restrict eavesdroppers, quantum cryptography focuses on the physics of information. The security of these transmissions is guaranteed by the inviolability of the laws of quantum mechanics. The quantum cryptography is based on two important elements of quantum mechanics-the Heisenberg Uncertainty principle and the principle of photon polarization. This paper summarizes the current state of quantum cryptography and review of quantum key distribution via the BB84 protocol and its use to secure data. Paper also summarizes a review on whether Quantum cryptography is really better and should replace conventional or modern cryptographic techniques.

KEYWORDS: CC V/S QC, Heisenberg Uncertainty Principle, Photon Polarization, QKD Protocol, Quantum Cryptography

INTRODUCTION

Modern network security violations involve accessing unauthorized data in an illegal manner. The major concern is that most attacks involve secret manner access to information resources, and organizations are not aware of illegal access to their data and information asset. For example, in one of the optical network serving a financial organization was found to be attacked and the information was tapped just before their earning release in the year 2003. In fact, CSI/FBI computer and security violation survey reports that 80% of respondents lost money because of computer breaches. This showed that asset in the form of data is actually insecure over internet and other mediums and there is great need to protecting everything from business e-mail to bank transactions and internet shopping. Hence cryptography was used for protecting the same. The classical and modern cryptographic techniques involved or are based on mathematical techniques and one way functions [5, 4, 11]. However the progress and development in optical computer will be threat to security and the system will not be secure any more. The most famous and trustable RSA algorithm of cryptography will fail to serve the security of the system [7, 14]. Moreover, if this happens then previous and past secrets may also get revealed. The above shortcomings has given a need of a new direction and which in turn led to the development of new technique called Quantum Cryptography (QC) [1,2,3,13].

QUANTUM CRYPTOGRAPHY

QC is an emerging technology in which two parties can communicate over network securely. It enables users to

securely develop secret keys, share them as well as to detect eavesdropping. The security of quantum key distribution relies on the inviolable laws of quantum mechanics [1,2]. The two laws that support and are backbone of QC are Heisenberg Uncertainty principle and principle of photon polarization. Heisenberg uncertainty principle states that it is not possible to measure the quantum state of any system without distributing that system [4, 12, 13]. Photon polarization states that an eavesdropper cannot copy unknown qubits i.e. unknown quantum states due to no cloning theorem [10]. Remember QC does not provide any encryption techniques. Instead it just provides a method to agree upon a secret key. Further this key can be used for standard encryption algorithms to achieve security goals.

Thus quantum cryptography allows a bit string to be agreed between two communications parties without having two parties to meet face to face and yet that two parties can be sure with a high confidence that the agreed bit string is exclusively shared between them. BB84 is the first QC protocol that was developed by Charles Bennett and Gills Brassard in 1984 allows two parties, conventionally "Alice" and Bob", to establish a secret common key sequence using polarized photons. Let each of the photon states are denoted by the following four symbols: —, |, ⁄, \,. Where the first two photon states are emitted by a rectilinear (+) polarizer and other two by diagonal(X) polarizer [1]. If Alice sends random sequence of photons: x++xx+xx+x whose binary equivalent is 100111010. Since Bob uses his detection randomly, some of his detection filter may not match with that of the used by Alice. Only Bits for which Alice polarization matches with Bobs are consider as final secret key (00110 in this ex.). This is depicted in Figure 1

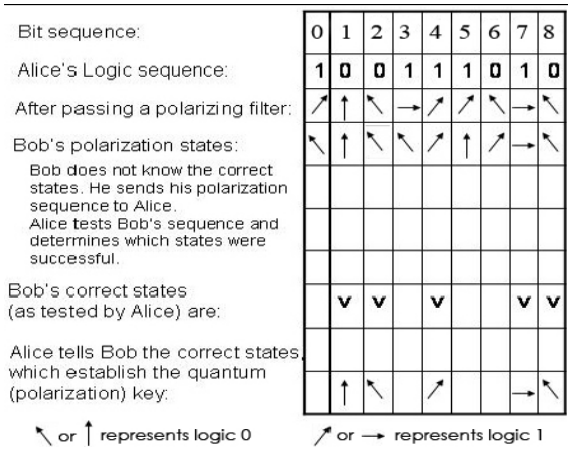

Figure 1: Key Agreement Using QC

This secret key is further used as encryption key for standard algorithms.

CC OVER QC

We have seen that QC provides a mechanism for generating a secret key and exchange securely, but the question arises will CC lose its place and will QC be able to sustain on its own? 'Definitely not', here are the advantages that CC holds over QC which assures it a permanent place in the future.

Medium Independent: The security with CC purely depends on the mathematical complexity, hence key and data exchange can happen over any media where traditional means of communication is considered possible.

Identity: Internet network is vey huge with millions of users along with thousands of hackers, one would always eager to know as who is the sender of the information and whether it is from the legitimate sender or not. Since algorithms can be implemented in CC, powerful solutions like the Digital Signatures have been developed.

Life Expectancy: Moors law states that computational power doubles approximately every 18months and we also see that the cost of computation is reducing drastically with time. Due to this an algorithm using an n-bit key which is proving secure now may not be safe in a few years from now, refer table 1.

Table 1: Some Examples

	Bit Length	Expected Lift Time
Triple Key DES	112	Through 2030
256-bit AES	256	Beyond 2030
DSA (p=7680, q=384)	192	Beyond 2030
DSA (p=2048, q=224)	128	Through 2030
SHA-512	256	Beyond 2030
SHA-224	112	Through 2030

This is seen as one of the biggest drawbacks in CC. But increased computational power is not only in the hands of Eve, but is also available to Alice and Bob. Thus with some gumption we can say that it's not a pitfall for CC. All that is required to increase the key size is better and affordable computational power. Thus when its year 2030 one can expect key size of 16,384-bits [6] or greater being processed at the same speed and cost thus ensuring security at least till year 2050, and this will go on. Processors at any time can do the forward 'one way' mathematics much faster than the reverse process and thus life time of an algorithm can be increased quite indefinitely, the only problem being the need for regular up-gradation.

Long Communication Range: The core of CC is mathematical complexity and distance of communication is not a limiting factor hence CC promises secure communication over millions of kilometres.

Multiple Platforms for Implementation: Both hardware and software implementation is possible when CC is used to for security. Hardware implementation is widely used for speeding up communication and also to make the algorithms tamper free [8]. Software implementation for communication is slow but has the flexibility of changing the key size at will. Such security especially security through software can only be handled using CC algorithms.

"I Don't Need a Reliable Courier"- CC: Courier reliability is not an issue in CC because its security bets only on the computational complexity. Thus even with full information of what is being sent; Eve will have to downtime and compute for thousands of years before he gets to know the plain text. This removes the need for exorbitant secure channels.

Key or Cipher Text Exchange in Complex Networks: Considering any network in existence now; we will find that everything network is highly interlinked and one is having a need to communicate using a shared channel. Key exchange in such integrated networks using CC is a cake walk.

What if Q Computing Becomes a Reality?: It is estimated that a 1024-bit RSA key could be broken with roughly 3000 qubits. Given that current Quantum Computers (Q Cmp) have below 10 qubits, public-key cryptography is safe for the foreseeable future, but this is not an absolute guarantee [9]. So what happens when a 3000-qubit Q Cmp becomes a reality? This issue is analogous to the one discussed under the 'Life Expectancy' i.e. use the computational resource of a Q Cmp to implement complex algorithms to make cracking difficult for another Q Cmp. Example, if Alice is using RSA Algorithm, then he can generate very large primes (there is no upper limit for primes) and process them quickly to exchange the cipher text with Bob. These primes having been generated by a Q Cmp will be large enough to trouble another Q Cmp try to crack the information. It's a well known fact that multiplying two primes is always easier than factoring the product. In fact with the upcoming of faster processors, new computationally demanding algorithms may be

discovered and implemented in future without the worry of slowing down the communication process.

CONCLUSIONS

The Quantum Cryptography is a technique use to agree on a secret key securely. The ability to detect the presence of eavesdropper is one of the important feature of QC. However there are certain challenges before QC can be widely used in the market. This includes developing more advanced hardware to enable higher quality and longer transmission distances for quantum key exchange. This paper work has also mentioned about advantages of classical cryptography over quantum cryptography. From the comparative study of classical and quantum cryptography we can conclude that the advances in technology will remain a driving force in the development of quantum cryptography and hence for few more years to come it will be classical cryptography having superior demand in market over quantum cryptography.

REFERENCES

1. Bennett, Ch. H., & Brassard, G., "Quantum cryptography: public key distribution and coin tossing", IEEE Conference on Computer, Systems, and Signal Processing, 1984, pp. 175-90.
2. Bennett, C. H., "Quantum cryptography using any two non-orthogonal states". Physics Review Letter, 68, 1992 p.3121-3124.
3. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J., "Experimental quantum cryptography". Journal of Cryptology, 5(1), 1992 p. 3-28.
4. Bruss, D., Erdelyi, G., Meyer, T., Riege, T., & Rothe, J., "Quantum cryptography: A survey". ACM Computing Surveys, 39(2), 2007, p. 1-27.
5. Buchmann, J., May, A., & Vollmer U., "Perspective for cryptographic long-term security". Communications of ACM. 49(9), 2006, p. 50-56.
6. R.L. Rivest, "Dr. Ron Rivest on the Difficulty of Factoring," Cipher text: The RSA Newsletter, v. 1, n. 1, Fall 1993, pp. 6, 8.
7. Buchmann, J., May, A., & Vollmer U., " Perspective for cryptographic long-term security" Communications of ACM,Vol.49, No. 9, 2006, pp. 50-56.
8. W.F. Ehrsam, C.H.W. Meyer, and W.L. Tuchman, "A Cryptographic Key Management Scheme for Implementing the Data Encryption Standard," IBM Systems Journal, v. 17, n. 2, 1978, pp. 106–125.
9. Information Security Management Handbook By Harold F. Tipton, Micki Krause
10. Wootters, W. K., & Zurek, W. H., "A single quantum cannot be cloned". Nature, 299, 1982, p. 802.
11. Simmon, G. J,"Symmetric and asymmetric encryption", ACM Computing Surveys, 11(4), 1979, p. 305- 330.
12. Hrg, D., Budin, L., & Golub, M.,"Quantum cryptography and security of information systems", *IEEE Proceedings of the 15th Conference on Information and Intelligent System*, 2004, p. 63-70.
13. Papanikolaou, N., "An introduction to quantum cryptography", *ACM Crossroads Magazine*, Vol.11 No.3, 2005, pp. 1-16.